İTÜ
LİSANSÜSTÜ DERS KATALOG FORMU
(GRADUATE COURSE CATALOGUE FORM)

Dersin Adı	**Course Name**
Bilgi ve Bilgisayar Güvenliği	Information and Computer Security

Kodu (Code)	**Yarıyılı (Semester)**	**Kredisi (Local Credits)**	**AKTS Kredisi (ECTS Credits)**	**Ders Seviyesi (Course Level)**
BGK 503E	Güz/Bahar (Fall/Spring)	3	7,5	Y.L. (M.Sc.)

Lisansüstü Program (Graduate Program)	Bilgi Güvenliği Mühendisliği ve Kriptografi (Cybersecurity Engineering and Cryptography)		
Dersin Türü (Course Type)	Seçmeli (Elective)	**Dersin Dili (Course Language)**	İngilizce/Türkçe (English/Turkish)

Dersin İçeriği **(Course Description)** *30-60 kelime arası*	Bilgi, güvenlik ve bilgisayar güvenliği konularının tanıtımı, Bilgi Güvenliği, Bilgi güvenliği sorunları, Güvenlik sağlama yöntemleri, Verileri gizleme yöntemleri: Şifreleme yöntemleri, Şifreleme yöntemlerinin temelleri ve çeşitleri, Simetrik ve asimetrik şifreleme yöntemleri, Doğrusallık, Kimlik asıllama, e-imza, Açık anahtarlama altyapısı, Saldırı yöntemleri ve karşı önlemler, Güvenlik sınıflamaları ve standartlar
	Introduction to information, security and computer security. Information security. Threats and defenses of information security. Confidentiality methods: encryption, fundamentals of encryption methods and classes. Symmetric and asymmetric encryption. Linearity, authentication, electronic signature, PKI. Attack methods and counter measurements. Classifications and standards of security.
Dersin Amacı **(Course Objectives)** *Maddeler halinde 2-5 adet*	• Bilgi ve bilgisayar güvenliği konusunu tanıtmak • Program içinde pek çok derse temel oluşturacak kavramları açıklamak
	• Introducing data and computer security • To give basic definitions and concepts that are fundamental for future courses
Dersin Öğrenme Çıktıları **(Course Learning Outcomes)** *Maddeler halinde 4-9 adet*	1. Öğrenciler bilgi ve bilgisayar güvenliği konusunu tanıyacaklardır. 2. Öğrenciler şifreleme yöntemleri hakkında temel bilgiye sahip olacaklardır. 3. Öğrenciler temel saldırıları ve bunlardan korunma yöntemlerini öğreneceklerdir. 4. Öğrenciler bilgisayar güvenliğinin temel kavramlarını bileceklerdir.
	1. To introduce data and computer security 2. To introduce fundamentals of encryption methods 3. To introduce the basics of attacks and counter measurements 4. To introduce basic concepts of computer security

Kaynaklar **(References)** *En önemli 5 adedini belirtiniz*	1. Computer Security, 3rd Ed., Dieter Gollmann, 2011, Wiley. 2. Computer Security: Principles and Practice, 2nd Ed. William Stallings, Lawrie Brown, 2011, Prentice Hall. 3. Computer and Information Security Handbook, 2nd Ed., John R. Vacca, 2013, Morgan Kaufmann. 4. Information Security The Complete Reference, 2nd Ed., Mark Rhodes-Ousley, 2013, McGraw-Hill Osborne Media. 5. Principles of Information Security, 4th Ed., Michael E. Whitman, Herbert J. Mattord, 2011, Cengage Learning.		
Ödevler ve Projeler **(Homework & Projects)**	1 Dönem Ödevi 1 Term Paper		
Laboratuar Uygulamaları **(Laboratory Work)**	-- --		
Bilgisayar Kullanımı **(Computer Use)**	-- --		
Diğer Uygulamalar **(Other Activities)**	-- --		
Başarı Değerlendirme Sistemi **(Assessment Criteria)**	**Faaliyetler (Activities)**	**Adedi* (Quantity)**	**Değerlendirmedeki Katkısı, % (Effects on Grading, %)**
	Yıl İçi Sınavları (Midterm Exams)	1	% 30 (30 %)
	Kısa Sınavlar (Quizzes)	-	-
	Ödevler (Homework)	-	-
	Projeler (Projects)	-	-
	Dönem Ödevi/Projesi (Term Paper/Project)	1	% 30 (30%)
	Laboratuar Uygulaması (Laboratory Work)	-	-
	Diğer Uygulamalar (Other Activities)	-	-
	Final Sınavı (Final Exam)	1	% 40 (40%)

*****Yukarıda Belirtilen Sayılar Minimum Olup Yerine Getirilmesi Zorunludur.

DERS PLANI

Hafta	Konular	Dersin Çıktıları
1	Bilgi, güvenlik, entropi kavramları, bilgisayar güvenliğinin kapsamı	
2	Bilgi güvenliği sorunları, güvenlik sağlama yöntemleri	
3	Şifreleme yöntemleri: Şifrelemenin temelleri ve çeşitleri	
4	Bakışımlı ve bakışımsız şifreleme yöntemleri	
5	Veri bütünlüğü ve öz alma yöntemleri	
6	Elektronik imza, sertifikalar ve açık anahtar altyapısı	
7	Asıllama	
8	Veri gizleme	
9	Biyometrik ve istatistik yöntemler	
10	Saldırı yöntemleri ve önlemler	
11	Güvenlik sınıflamaları ve standartları	
12	Erişim denetimi	
13	Erişim modelleri	
14	Güvenlik sertifikasyonu	

COURSE PLAN

Weeks	Topics	Course Outcomes
1	Concept of information, security, entropy and computer security	
2	Threats and defences of information security	
3	Encryption methods: fundamentals and classes of encryption	
4	Symmetric and asymmetric encryption methods	
5	Data integrity and hash methods	
6	Electronic signatures, electronic certificates, and PKI	
7	Authentication	
8	Data hiding	
9	Biometric and statistical methods	
10	Attacks and counter measures	
11	Security classes and standards	
12	Access control	
13	Access models	
14	Security certification	

Dersin Bilgi Güvenliği Mühendisliği ve Kriptografi Yüksek Lisans Programıyla İlişkisi

	Programın mezuna kazandıracağı bilgi, beceri ve yetkinlikler (programa ait çıktılar)	Katkı Seviyesi		
		1	2	3
i.	Lisans düzeyi yeterliliklerine dayalı olarak, Bilgi Güvenliği Mühendisliği ve Kriptografi alanında bilgilerini uzmanlık düzeyinde geliştirebilme ve derinleştirebilme (yeterli bilgi birikimi) (bilgi).	X		
ii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının ilişkili olduğu disiplinler arası etkileşimi kavrayabilme (bilgi).		X	
iii.	Bilgi Güvenliği Kriptografi alanında edindiği uzmanlık düzeyindeki kuramsal ve uygulamalı bilgileri kullanabilme (beceri).			
iv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği bilgileri farklı disiplin alanlarından gelen bilgilerle bütünleştirerek yorumlayabilme ve yeni bilgiler oluşturabilme (beceri).	X		
v.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili karşılaşılan sorunları araştırma yöntemlerini kullanarak çözümleyebilme (beceri).			
vi.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uzmanlık gerektiren bir çalışmayı bağımsız olarak yürütebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
vii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili uygulamalarda karşılaşılan ve öngörülemeyen karmaşık sorunların çözümü için yeni stratejik yaklaşımlar geliştirebilme ve sorumluluk alarak çözüm üretebilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
viii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili sorunların çözümlenmesini gerektiren ortamlarda liderlik yapabilme (Bağımsız Çalışabilme ve Sorumluluk Alabilme Yetkinliği).			
ix.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında edindiği uzmanlık düzeyindeki bilgi ve becerileri eleştirel bir yaklaşımla değerlendirebilme ve öğrenmesini yönlendirebilme (Öğrenme Yetkinliği).		X	
x.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki güncel gelişmeleri ve kendi çalışmalarını, nicel ve nitel veriler ile destekleyerek, alanındaki ve alan dışındaki gruplara, yazılı, sözlü ve görsel olarak sistemli biçimde Türkçe ve/veya İngilizce olarak aktarabilme (İletişim ve Sosyal Yetkinlik).	X		
xi.	Sosyal ilişkileri ve bu ilişkileri yönlendiren normları eleştirel bir bakış açısı ile inceleyebilme, geliştirebilme ve gerektiğinde değiştirmek üzere harekete geçebilme (İletişim ve Sosyal Yetkinlik).	X		
xii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanının gerektirdiği düzeyde bilgisayar yazılımı ile birlikte bilişim ve iletişim teknolojilerini ileri düzeyde kullanabilme (İletişim ve Sosyal Yetkinlik).			X
xiii.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili verilerin toplanması, yorumlanması, uygulanması ve duyurulması aşamalarında toplumsal, bilimsel, kültürel ve etik değerleri gözeterek denetleyebilme ve bu değerleri öğretebilme (Alana Özgü Yetkinlik).		X	
xiv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanı ile ilgili konularda strateji, politika ve uygulama planları geliştirebilme ve elde edilen sonuçları, kalite süreçleri çerçevesinde değerlendirebilme (Alana Özgü Yetkinlik).			
xv.	Bilgi Güvenliği Mühendisliği ve Kriptografi alanında özümsedikleri bilgiyi, problem çözme ve/veya uygulama becerilerini, disiplinler arası çalışmalarda kullanabilme (Alana Özgü Yetkinlik).	X		
xvi.	Kendi çalışmalarını, Bilgi Güvenliği Mühendisliği ve Kriptografi alanındaki uluslararası platformlarda, yazılı, sözlü ve/veya görsel olarak aktarabilme (Alana özgü yetkinlik).	X		

1: Az, 2. Kısmi, 3. Tam

Relationship between the Course and Cybersecurity Engineering and Cryptography Graduate (MS) Curriculum

	Program Outcomes	Level of Contribution		
		1	2	3
i.	Developing and intensifying knowledge in Cybersecurity Engineering and Cryptography area, based upon the competency in the undergraduate level (sufficient knowledge) (knowledge).	X		
ii.	Grasping the inter-disciplinary interaction related to Cybersecurity Engineering and Cryptography area (knowledge).		X	
iii.	The ability to use the expert-level theoretical and practical knowledge acquired in Cybersecurity Engineering and Cryptography area (skill).			
iv.	Interpreting and forming new types of knowledge by combining the knowledge from Cybersecurity Engineering and Cryptography area and the knowledge from various other disciplines (skill).	X		
v.	Solving the problems faced in Cybersecurity Engineering and Cryptography area by making use of the research methods (skill).			
vi.	The ability to carry out a specialist study related to Cybersecurity Engineering and Cryptography area independently (Competence to work independently and take responsibility).			
vii.	Developing new strategic approaches to solve the unforeseen and complex problems arising in the practical processes of Cybersecurity Engineering and Cryptography area and coming up with solutions while taking responsibility (Competence to work independently and take responsibility).			
viii.	Fulfilling the leader role in the environments where solutions are sought for the problems related to Information Security Cryptography area (Competence to work independently and take responsibility)			
ix.	Assessing the specialist knowledge and skill gained through the study with a critical view and directing one's own learning process (Learning Competence).		X	
x.	Systematically transferring the current developments in Cybersecurity Engineering and Cryptography area and one's own work to other groups in and out of Cybersecurity Engineering and Cryptography area; in written, oral and visual forms in Turkish and/or English (Communication and Social Competency).	X		
xi.	Ability to see and develop social relationships and the norms directing these relationships with a critical look and the ability to take action to change these when necessary. (Communication and Social Competency).	X		
xii.	Using the computer software together with the information and communication technologies efficiently and according to the needs of Cybersecurity Engineering and Cryptography area (Communication and Social Competency).			X
xiii.	Paying regard to social, scientific, cultural and ethical values while collecting, interpreting, practicing and announcing processes of Cybersecurity Engineering and Cryptography area related data and the ability to teach these values to others (Area Specific Competency).		X	
xiv.	Developing strategy, policy and application plans concerning the subjects related to Cybersecurity Engineering and Cryptography ng area and the ability to evaluate the end results of these plans within the frame of quality processes (Area Specific Competency).			
xv.	Using the knowledge and the skills for problem solving and/or application (which are processed within the area) in inter-disciplinary studies (Area Specific Competency).	X		
xvi.	The ability to present one's own work within the international Cybersecurity Engineering and Cryptography environments orally, visually and in written forms (Area Specific Competency).	X		

1: Little, 2. Partial, 3. Full

Düzenleyen (Prepared by)	***Tarih (Date)***	***İmza (Signature)***
Prof. Dr. Eşref ADALI	31.03.2014	